Załącznik 1

Wymagania dotyczące systemu ochrony anty wirusowej z zaporą ogniową dla stacji roboczych.

1. Ochrona antywirusowa stacji roboczych:
   - Microsoft Windows Vista (32-bit i 64-bit)
   - Microsoft Windows 7 (32-bit i 64-bit)
   - Microsoft Windows 8 (32-bit i 64-bit)
   - Microsoft Windows 8.1 (32-bit i 64-bit)
   - Microsoft Windows 10
2. Ochrona antywirusowa wyżej wymienionego systemu monitorowana i zarządzana z pojedynczej, centralnej konsoli.
3. Komunikacja ochrony antywirusowej z serwerem zarządzania musi odbywać się za pomocą protokołu HTTPS.
4. Możliwość instalacji konsoli zarządzania niezależnie na kilku wybranych stacjach.
5. Polski interfejs użytkownika aplikacji ochronnej.

Wymagania dotyczące technologii:

1. Ochrona antywirusowa realizowana na wielu poziomach, tj.: monitora kontrolującego system w tle, modułu skanowania heurystycznego, modułu skanującego nośniki i monitora poczty elektronicznej, monitora ruchu http oraz moduł antyrootkitowy.
2. Co najmniej trzy różne silniki antywirusowe, funkcjonujące jednocześnie i skanujące wszystkie dane.
3. Oddzielny silnik skanujący do wykrywania niepożądanych aplikacji takich jak oprogramowanie typu „spyware", „adware", „keylogger”, „dialer”, „trojan”.
4. Aktualizacje baz definicji wirusów dostępne 24h na dobę na serwerze internetowym producenta, możliwa zarówno aktualizacja automatyczna programu oraz na żądanie, jak i ściągnięcie pliku offline ze strony producenta i ręczna aktualizacja na stacjach roboczych bez dostępu do Internetu.
5. Możliwość wywołania skanowania komputera na żądanie lub według harmonogramu ustalonego przez administratorów dla określonych grup klientów za pomocą centralnej konsoli lub lokalnie przez określonego klienta.
6. Możliwość wywołania skanowania komputera w określone dni i godziny tygodnia i miesiąca, a także po określonym czasie bezczynności komputera.
7. Możliwość wywołania skanowania podczas uruchamiania systemu operacyjnego lub po zalogowaniu użytkownika.
8. Aktualizacja definicji wirusów czy też mechanizmów skanujących nie wymaga zatrzymania procesu skanowania na jakimkolwiek systemie.

9. Mikrodefinicje wirusów – przyrostowe (inkrementalne) - pobieranie jedynie nowych definicji wirusów i mechanizmów skanujących bez konieczności pobierania całej bazy (na stację kliencką pobierane są tylko definicje, które przybyły od momentu ostatniej aktualizacji).
10. Możliwość pobierania aktualizacji definicji wirusów bezpośrednio z serwerów producenta, centralnej konsoli, dedykowanego proxy lub z innej stacji roboczej gdzie zainstalowane jest oprogramowanie antywirusowe.
11. Brak konieczności restartu systemu operacyjnego po dokonaniu aktualizacji mechanizmów skanujących i definicji wirusów.
12. Heurystyczna technologia do wykrywania nowych, nieznanych wirusów.
13. Wykrywanie niepożądanych aplikacji takich jak oprogramowanie typu „spyware", „adware", „keylogger", „dialer", „trojan", „rootkit".
14. Możliwość umieszczenia oprogramowania typu „spyware", „adware", „keylogger", „dialer", „trojan" w kwarantannie.
15. Ochrona pliku 'hosts' przed niepożądanymi wpisami.
16. Mechanizm centralnego zarządzania elementami kwarantanny znajdującymi się na stacjach klienckich.
17. Mechanizm określania źródeł ataków prowadzonych przy użyciu zagrożeń hybrydowych, takich jak Code Red i Nimda.
18. Obsługa plików skompresowanych obejmująca najpopularniejsze formaty w tym, co najmniej: ZIP JAR ARJ LZH TAR TGZ GZ CAB RAR BZ2 HQX.
19. Automatyczne usuwanie wirusów oraz oprogramowania typu malware i zgłaszanie alertów w przypadku wykrycia wirusa.
20. Logowanie historii akcji podejmowanych wobec wykrytych zagrożeń na stacjach roboczych. Dostęp do logów z poziomu GUI aplikacji.
21. Automatyczne uruchamianie procedur naprawczych.
22. Uaktualnienia definicji wirusów posiadają podpis cyfrowy, którego sprawdzenie gwarantuje, że pliki te nie zostały zmienione.
23. Średni czas reakcji producenta na nowy wirus poniżej 8 godzin, 24 godziny na dobę przez cały rok (24/7/365).
24. Automatyczne powiadomienie użytkowników oraz administratora o wykrytych zagrożeniach wraz z określeniem czy stacja robocza jest odpowiednio zabezpieczona.
25. Skanowanie przez program na komputerze klienckim przychodzącej i wychodzącej poczty elektronicznej bez konieczności instalowania dodatkowych programów/modułów.
26. Możliwość zablokowania wychodzącej wiadomości e-mail, jeżeli zostanie w niej wykryty zainfekowany załącznik.
27. Skanowanie przez program na komputerze klienckim, danych pobieranych i wysyłanych danych przy pomocy protokołu http.
28. Blokowanie przez program na komputerze klienckim określonego przez administratora rodzaju zawartości oraz nazwy lub rozszerzeń poszczególnych plików pobieranych przy pomocy protokołu http.
29. Skanowanie http oraz blokowanie zawartości może być deaktywowane dla witryn określonych, jako zaufane przez serwery reputacyjne producenta.
30. Automatyczna kwarantanna blokująca ruch przychodzący i wychodzący, włączająca się w momencie, gdy stacja robocza posiada stare sygnatury antywirusowe.
31. Wsparcie dla technologii Microsoft Network Access Protection (NAP).

32. Ochrona przeglądarki internetowej, w tym: blokowanie wyskakujących okienek, blokowanie ciasteczek (cookies), blokowanie możliwości zmian ustawień w IE, analiza uruchamianych skryptów ActiveX i pobieranych plików.
33. Ochrona podczas przeglądania sieci Internet na podstawie badania reputacji – moduł działający na bazie *Network Interceptor Framework* (niezależnie od rodzaju i wersji przeglądarki).
34. Możliwość ręcznego aktualizowania baz definicji wirusów poprzez odrębny plik wykonywalny dostarczony przez producenta.
35. Ochrona rejestrów systemowych, w tym odpowiedzialnych za konfigurację przeglądarki Internet Explorer, listę uruchamianych aplikacji przy starcie, przypisania rozszerzeń plików do zadanych aplikacji.
36. Kontrola oraz możliwość blokowania aplikacji próbujących uzyskać połączenie z Internetem lub siecią lokalną.
37. Osobista zapora ogniowa (tzw. personal firewall) z możliwością definiowania profili bezpieczeństwa możliwych do przypisania dla pojedynczej stacji roboczej lub grup roboczych.
38. Profile bezpieczeństwa zapory ogniowej zawierają predefiniowane reguły zezwalające na bezproblemową komunikację w sieci lokalnej.
39. Możliwość automatycznego przełączenia profilu bezpieczeństwa zapory ogniowej po spełnieniu określonych warunków (np. zmiana adresacji karty sieciowej na stacji roboczej)
40. Użytkownik podczas próby przejścia na witrynę znajdująca się w zablokowanej przez Administratora musi zostać powiadomiony o nałożonej na niego blokadzie komunikatem w przeglądarce internetowej.
41. Możliwość blokowania zapytań DNS do witryn sklasyfikowanych, jako niebezpieczne lub podejrzane.
42. Możliwość zezwolenia na zapytania DNS tylko do witryn sklasyfikowanych, jako zaufane.
43. Brak konieczności restartu komputera po zainstalowaniu aplikacji w środowisku Windows Vista/7/8/8.1
44. Moduł kontroli urządzeń zapewniający możliwość zezwolenia lub zablokowania dostępu do urządzeń zewnętrznych (np. napędy USB, urządzenia bluetooth, czytniki kart pamięci, napędy CD/DVD, stacje dyskietek).
45. Moduł kontroli urządzeń zarządzany z poziomu konsoli centralnego zarządzania.
46. Moduł kontroli urządzeń umożliwia dodanie ‘zaufanego urządzenia’ poprzez podanie jego identyfikatora sprzętu.

Wymagania dotyczące systemu zarządzania centralnego:

1. System centralnego zarządzania może być zainstalowany na wersjach serwerowych Microsoft Windows oraz Linux.
2. Instalacja sytemu centralnego zarządzania dla Microsoft Windows musi wspierać następujące wersje systemów operacyjnych:
   - Windows Server 2008 SP1 32-bit : Standard, Enterprise, Web Server
   - Windows Server 2008 SP1 64-bit: Standard, Enterprise, Web Server, Small Business Server, Essential Business Server
   - Windows Server 2008 R2: Standard, Enterprise, Web Server
   - Windows Server 2012: Essentials, Standard, Datacenter

- Windows Server 2012 R2: Essentials, Standard, Datacenter
- Windows 2016 ready

3. Instalacja sytemu centralnego zarządzania dla Linux musi wspierać następujące wersje systemów operacyjnych:
   - Red Hat Enterprise Linux 5 32/64-bit
   - Red Hat Enterprise Linux 6 32/64-bit
   - Red Hat Enterprise Linux 7 32/64-bit
   - CentOS 6 32/64-bit
   - CentOS 7 32/64-bit
   - SuSE Linux Enterprise Server 10 32/64-bit
   - SuSE Linux Enterprise Server 11 32/64-bit
   - SuSE Linux Enterprise Desktop 11 32/64-bit
   - openSUSE 13.2 32/64-bit
   - Debian GNU Linux 7 (Wheezy) 32/64-bit
   - Debian GNU Linux 8 (Jessie) 32/64-bit
   - Ubuntu 12.04 (Precise Pangolin) 32/64-bit
   - Ubuntu 14.04 (Trusty Tahr) 32/64-bit
   - Ubuntu 16.04 (Xenial Xerus) 32/64-bit
4. Konsola zarządzania umożliwia eksport pakietu instalacyjnego dla klienta w formacie Microsoft Installer (MSI) i JAR lub też bezpośrednią instalację zdalną nienadzorowaną.
5. Narzędzie instalacyjne musi sprawdzać istnienie poprzednich wersji oprogramowania. W przypadku znalezienia poprzedniej wersji instalator powinien pozostawić ustawienia użytkownika, usunąć starsze oprogramowanie z klienta lub serwera i instalować nowe wersję.
6. Pełna administracja konfiguracją i monitorowanie stacji roboczych i serwerów plików za pomocą konsoli administracyjnej (centralna instalacja, konfiguracja w czasie rzeczywistym, zarządzanie, raportowanie i administrowanie oprogramowaniem).
7. Komunikacja pomiędzy serwerem centralnego zarządzania a stacjami roboczymi musi być zaszyfrowana lub sygnowana stosownymi kluczami prywatnymi i publicznymi.
8. Scentralizowane blokowanie i odblokowywanie dostępu użytkownika do zmian konfiguracyjnych oprogramowania klienckiego, konsola pozwala na zdalne zarządzanie wszystkimi ustawieniami klienta.
9. Administratorzy muszą mieć możliwość tworzenia logicznych grup klientów i serwerów, w celu zarządzania oraz wymuszania określonych dla grupy zasad bezpieczeństwa.
10. Centralna konsola administracyjna musi umożliwiać przenoszenie klientów z jednej grupy do drugiej z możliwością zachowania ustawień lub dziedziczenia ustawień grupy.
11. Możliwość zmiany ustawień dla poszczególnych grup, umożliwienie administratorom zarządzania poszczególnymi klientami i funkcjonalnymi grupami klientów (tworzenie grup klientów).
12. Tworzenie grup, zdalne instalowanie oprogramowania oraz wymuszanie stosowania określonych zasad i ustawień na klientach.
13. Możliwość importu struktury drzewa z Microsoft Active Directory.

14. Możliwość tworzenia reguł synchronizacji z Microsoft Active Directory umożliwiających automatyczną synchronizację klientów z aktualnie istniejącymi grupami komputerów
15. Możliwość tworzenia reguł powiadamiania o nowych, niezarządzanych klientach w Microsoft Active Directory.
16. Możliwość blokowania wszystkich ustawień konfiguracyjnych stacji roboczych w celu uniemożliwienia ich modyfikacji przez użytkowników.
17. Możliwość definiowania harmonogramów lub częstotliwości automatycznego pobierania aktualizacji definicji wirusów od producenta oprogramowania przez serwer zarządzający.
18. Funkcja przechowywania i przekazywania danych umożliwiająca przechowywanie przez klientów danych dotyczących zdarzeń, w sytuacji, jeśli nie mogą oni uzyskać połączenia z serwerem zarządzania. Dane muszą być przesyłane do serwera zarządzania podczas kolejnego połączenia.
19. Możliwość włączania/wyłączania wyświetlania komunikatów o znalezionych wirusach na wybranych stacjach klienckich.
20. Umożliwienie administratorom na audyt sieci, polegający na wykryciu niechronionych węzłów narażonych na ataki wirusowe.
21. Automatyczne wykrywanie i usuwanie oprogramowanie innych wiodących producentów systemów antywirusowych podczas instalacji.
22. Automatyczne uaktualnianie bazy definicji wirusów oraz mechanizmów skanujących nie rzadziej, niż co 7 dni (zalecane codzienne aktualizacje).
23. Automatyczne pobieranie przez program antywirusowy klienta zaktualizowanych definicji wirusów, jeśli aktualnie przechowywane pliki są przestarzałe.
24. Możliwość eksportu raportów z pracy systemu do pliku HTML.
25. Możliwość natychmiastowej aktualizacji przez serwer definicji wirusów na stacjach klienckich.
26. Możliwość uruchomienia aktualizacji stacji roboczych i serwerów przez użytkowników „na żądanie”.
27. Program musi pozwalać administratorowi na określenie reakcji w przypadku wykrycia wirusa.
28. Program musi pozwalać na określenie obszarów skanowania, tj.: pliki, katalogi, napędy lokalne i sieciowe.
29. Program musi pozwalać na skanowanie pojedynczych plików przez dodanie odpowiedniej opcji do menu kontekstowego (po kliknięciu prawym przyciskiem myszy).
30. Program musi pozwalać na określenie typów skanowanych plików, momentu ich skanowania (otwarcie, modyfikacja) oraz na wykluczenie ze skanowania określonych folderów.
31. Dedykowany system raportowania dostępny przez przeglądarkę internetową umożliwiający podgląd statystyk dotyczących wykrytych wirusów, przeprowadzonych ataków, zainstalowanego oprogramowania oraz statystyk połączenia stacji klienckich.
32. System raportowania umożliwiający wysyłanie raportów poprzez pocztę elektroniczną zgodnie z harmonogramem określonym przez administratora.
33. Zarządzanie zdarzeniami i raportowanie – natychmiastowe alarmowanie o aktywności wirusów w administrowanej sieci na kilka sposobów: poczta

elektroniczna, powiadomienia przez SNMP, raportowanie do dziennika systemowego, raportowanie do systemu centralnego zarządzania.

34. Możliwość przekierowania alertów bezpośrednio do serwera Syslog.
35. Możliwość tworzenia wielu kont dostępu do systemu centralnego zarządzania dla różnych użytkowników (w tym możliwość nadaniu danemu użytkownikowi ograniczonych praw).
36. System umożliwiający wykonanie pełnej kopii bazy danych systemu zarządzania centralnego bez konieczności ręcznego wyłączania programu.
37. Pełna kopia bazy danych systemu zarządzania centralnego może być wykonywana automatycznie zgodnie z harmonogramem określonym przez administratora.
38. Administrator ma możliwość określenia liczby kopii bazy danych, jaka będzie przetrzymywana.
39. Możliwość wygenerowania danych diagnostycznych z podpiętych komputerów za pomocą konsoli zarządzającej.
40. Możliwość bezpośredniego pobrania z komputera danych diagnostycznych z poziomu konsoli zarządzającej.